UNITED STATES DISTRICT COURT

for the
Western District of Virginia

In the Matter of the Search of
*(Briefly describe the property to be searched
or identify the person by name and address)*

Information associated with smust41@hotmail.com that
is stored at the premises controlled by Microsoft (MSN)

)
)
)
)
)
)
)

Case No. 7:13MJ107

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SMUST41@HOTMAIL.COM - stored at One Microsoft Way, Redmond, Washington, 98052-6399

located in the _____ Western _____ District of _____ Virginia _____ , there is now concealed *(identify the person or describe the property to be seized):*

*** PLEASE SEE ATTACHMENT A ***

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more):*

☑ evidence of a crime;

☑ contraband, fruits of crime, or other items illegally possessed;

☑ property designed for use, intended for use, or used in committing a crime;

☑ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. Section 3146	Violating the terms and conditions of Bond

The application is based on these facts:

*** PLEASE SEE ATTACHMENT B ***

☑ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

_____
Applicant's signature

Marla O'Brien CI-DUSM
Printed name and title

Sworn to before me and signed in my presence.

Date: September 10, 2013

_____
Judge's signature

City and state: Roanoke, Virginia

Honorable Robert S. Ballou
Printed name and title

CLERK'S OFFICE U.S. DIST. COURT
AT ROANOKE, VA
FILED

SEP 10 2013

JULIA C. DUDLEY, CLERK
BY: _____
DEPUTY CLERK

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
SMUST41@HOTMAIL.COM THAT IS
STORED AT PREMISES CONTROLLED BY
MICROSOFT (MSN)

Case No. 7:13MJ107

Filed Under Seal

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Marla O'Brien, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1.   I make this affidavit in support of an application for a search warrant for

information associated with email account smust41@hotmail.com a certain account that is stored

at premises of and controlled by Microsoft (MSN), an e-mail provider headquartered at One

Microsoft Way, Redmond, Washington, 98052-6399. The information to be searched is

described in the following paragraphs and in Attachment A. This affidavit is made in support of

an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and

2703(c)(1)(A) to require Microsoft (MSN) to disclose to the government copies of the

information (including the content of communications) further described in Section I of

Attachment B. Upon receipt of the information described in Section I of Attachment B,

government-authorized persons will review that information to locate the items described in

Section II of Attachment B.

2.   I am a Deputy U.S. Marshal with the U.S. Marshals Service and have been since

May, 2003. My duties as it pertains to this position include the location and apprehension of

federal and state fugitives and the investigation of various crimes against the United States of

America. I am experienced in locating and apprehending known fugitives as well as prosecuting criminal cases that are a result of fugitive investigations.

3.   This affidavit is intended to show that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4.   Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 3146 have been committed by Osama Mahmud Mustafa. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband or fruits of these crimes further described in Attachment B.

JURISDICTION

5.   This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court, Federal District Court for the United States within the Western District of Virginia, Roanoke Division is a district court of the United States that– has jurisdiction over the offense being investigated, 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

Osama Mahmud Mustafa was admitted to federal bond on or about June 27, 2012 by Federal Magistrate Court Judge Robert S. Ballou within the Western District of Virginia. The conditions of Mustafa's bond were that he shall appear for all court appearances as required. Mustafa received notice from the federal courts within the Western District of Virginia, Roanoke Division on or about August 21, 2013, requiring him to appear before a federal court judge on August 30, 2013.

2

On August 28, 2013, a federal arrest warrant was issued for Osama Mahmud Mustafa for violating the terms and conditions of his bond set forth by Magistrate Judge Robert S. Ballou within the Western District of Virginia, Roanoke Division. The warrant was received by the U.S. Marshals Service on this same date. On August 28, 2013, and after reviewing evidence provided by the Federal Probationer's office, it was evident to law enforcement that Mustafa had removed his gps electronic monitoring device that was affixed to his ankle on or about August 27, 2013. The removal of the device from Mustafa's person violated the terms and conditions of his bond and at that point his whereabouts became unknown. These circumstances prompted the issuing of a federal warrant for Mustafa's arrest as mentioned above. U.S. Marshals observed that within the evidence provided by federal probation, the gps monitoring device had been sitting in the same place for approximately 24 hour. The evidence provided by federal probation indicated that the location of the device was off Interstate 10 Westbound near Marianna, Florida.

On August 28, 2013, law enforcement received information that indicated Mustafa had rented a vehicle from Dollar/Thrifty Rental located at the Tampa, Florida international airport on August 26, 2013. This same vehicle was found on August 28, 2013 abandoned off Interstate 10 Westbound mile marker 136 on a dirt road.

On or about August 30, 2013, Deputy U.S. Marshals located the gps electronic monitoring device on or near Interstate 10 Westbound. The device was found lying just off Interstate 10 and was approximately 3 miles from where the abandoned rental vehicle had been located on August 28, 2013.

Over the next several days of the investigation into the whereabouts of Mustafa, a confidential source, an entity known and used in the normal course of criminal investigations conducted by the U.S. Marshals Service, indicated that Mustafa used an email account of

3

smust41@hotmail.com to book an on-line hotel reservation, via the use of Hotwire.com, at the Ramada Inn Roanoke on August 24, 2013. The confidential source that was used in this investigation has been used in several other criminal investigations conducted by the U.S. Marshals Service and is found to be a creditable and reliable source and tool used in law enforcement's endeavors to locate known fugitives.

On or about September 4, 2013, U.S. Marshals went to that same hotel to verify the reservation and to obtain any information related to Mustafa's reservation. Hotel management indicated that the account registered under Osama Mustafa was charged for a no-show on the reservation. Hotel management indicated that the account information, although reserved under Osama Mustafa, was paid for by Hotwire.

There is reason to believe that the email account to be searched, smust41@hotmail.com, could still be in use by Mustafa to conduct transactions or exchange information that would continue to aid and assist in his flight to avoid further prosecution by the Government of the United States. It is further believed, based on training and experience, that email accounts are used to communicate with confederates or those assisting in flight and believed to contain pertinent information as to those communications with such confederates.

6. In general, an e-mail that is sent to a Microsoft (MSN) subscriber is stored in the subscriber's "mail box" on Microsoft (MSN) servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Microsoft (MSN) servers indefinitely. Even if the subscriber deletes the e-mail, it may continue to be available on Microsoft (MSN) servers for a certain period of time.

4

BACKGROUND CONCERNING E-MAIL

7.   In my training and experience, I have learned that Microsoft (MSN) provides a variety of on-line services, including electronic mail ("e-mail") access, to the public. Microsoft (MSN) allows subscribers to obtain e-mail accounts at the domain name smust41@hotmail.com, like the e-mail account listed in Attachment A. Subscribers obtain an account by registering with Microsoft (MSN). During the registration process, Microsoft (MSN) asks subscribers to provide basic personal information. Therefore, the computers of Microsoft (MSN) are likely to contain stored electronic communications (including retrieved and un-retrieved e-mail for Microsoft (MSN) subscribers and information concerning subscribers and their use of Microsoft (MSN) services, such as account access information, e-mail transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

8.   A Microsoft (MSN) subscriber can also store with the provider files in addition to e-mails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to e-mails), and other files, on servers maintained and/or owned by Microsoft (MSN). In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.

9.   In my training and experience, e-mail providers generally ask their subscribers to provide certain personal identifying information when registering for an e-mail account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of

5

payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

10. In my training and experience, e-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

11. In my training and experience, in some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

6

CONCLUSION

12.   Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Microsoft (MSN) who will then compile the requested records at a time convenient to it, there exist reasonable cause to permit the execution of the requested warrant at any time in the day or night.
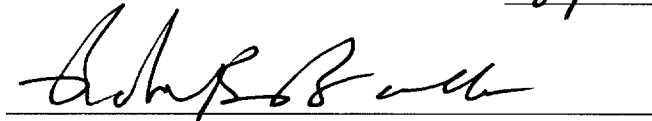
REQUEST FOR SEALING

13.   I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,

Marla O'Brien
Deputy U.S. Marshal

Subscribed and sworn to before me on _____, 2013

Honorable Robert S. Ballou
UNITED STATES MAGISTRATE JUDGE

7

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with email account smust41@hotmail.com which is stored at the premises of and controlled by Microsoft (MSN), a company that accepts service of legal process at One Microsoft Way, Redmond, Washington, 98052-6399 or by fax (425) 708-0096 or fax (425) 727-3490.

ATTACHMENT B

Particular things to be seized

I.   Information to be disclosed by Microsoft (MSN) (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) for August 1, 2013 through September 10, 2013 the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a.   The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;

b.   All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session

times and durations, the date on which the account was created, the length of service, the IP

address used to register the account, log-in IP addresses associated with session times and dates,

account status, alternative e-mail addresses provided during registration, methods of connecting,

log files, and means and source of payment (including any credit or bank account number);

    c.   The types of service utilized;

    d.   All records or other information stored at any time by an individual using the

account, including address books, contact and buddy lists, calendar data, pictures, and files;

    e.   All records pertaining to communications between the Provider and any person

regarding the account, including contacts with support services and records of actions taken.

II.   **Information to be seized by the government**

    All information described above in Section I that constitutes fruits, contraband,

evidence and instrumentalities of violations of **18 U.S.C. § 3146** those violations involving

Osama Mahmud Mustafa and occurring after August 27, 2013, including, for each account or

identifier listed on Attachment A, information pertaining to the following matters:

    a.   Electronic mail and other records relating to discussions between Osama Mustafa

about plans to fail to appear or flee; electronic mail or other records as to preparatory steps to

flight; electronic mail and other records relating to financial or material support provided in

preparation for or during flight by Osama Mustafa; electronic mail and other records as to

communication with confederates who may have assisted Osama Mustafa with flight or provided

support in preparation for or during flight; and electronic mail and other records showing the

location of Osama Mustafa during preparatory steps to flight and during and following the

commission of the offense.

b.   Information relating to who created, used, or communicated with the account, including records about their identities and whereabouts.

3

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Microsoft Corporation, and my official title is _____. I am a custodian of records for Microsoft Corporation. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Microsoft Corporation, and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a.   all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b.   such records were kept in the ordinary course of a regularly conducted business activity of Microsoft Corporation; and

c.   such records were made by Microsoft Corporation as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

_____   _____
Date   Signature